20-P

DEPARTMENT OF COMMERCE

15 CFR Part 7 [Docket No. 230125-0025]

RIN 0605-AA62

Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications

AGENCY: U.S. Department of Commerce

ACTION: Final rule.

SUMMARY: On November 26, 2021, the Department of Commerce (Department) published a Notice of Proposed Rulemaking (NPRM) proposing to amend Department regulations, "Securing the Information and Communications Technology Supply Chain," to implement provisions of Executive Order 14034, "Protecting Americans' Sensitive Data from Foreign Adversaries" (E.O. 14034). This final rule responds to, and adopts changes based on, the comments received to the NPRM. Consistent with the factors enumerated in E.O. 14034, the final rule amends the Securing the Information and Communications Technology Supply Chain regulations to provide additional criteria that the Secretary may consider when determining whether ICTS transactions involving connected software applications present undue or unacceptable risks (as those terms are defined in the regulations). The final rule also adds definitions for "end-point computing devices" and "via the internet" for the purposes of this rule to clarify the definition of connected software applications provided in E.O. 14034.

DATES: This rule is effective [Insert date 30 days after publication in the FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: Katelyn Christ, U.S. Department of Commerce, telephone: 202-482-3506, email: Katelyn.Christ@bis.doc.gov.

SUPPLEMENTARY INFORMATION:

I. Background

On January 19, 2021, the Department published an interim final rule (the Supply Chain Rule) to implement Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain" (E.O. 13873). The Supply Chain Rule established the Department regulations at title 15 of the Code of Federal Regulations (CFR) part 7, "Securing the Information and Communications Technology and Services Supply Chain" (part 7). These regulations set out procedures by which the Secretary of Commerce (Secretary), in consultation with the appropriate heads of other executive departments and agencies, reviews transactions involving information and communications technology and services (ICTS) that is designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries to determine whether those transactions present certain undue or unacceptable risks to the United States or U.S. persons. ICTS transactions include, as noted in 15 CFR 7.2, among other things, "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download."

On November 26, 2021, the Department published an NPRM seeking comments on amendments to Part 7 incorporating provisions of E.O. 14034 (86 FR 67379). Specifically, consistent with E.O. 14034, the NPRM proposed to add "connected software applications" to the range of ICTS transactions the Department can review under the regulations in Part 7. The Department proposed this addition given that the increased use of such connected software applications continues to potentially threaten the national security, foreign policy, and economy of the United States. E.O. 14034 also listed criteria that the Department should consider when evaluating the risks of any ICTS transaction involving "connected software applications."

Specifically, the NPRM proposed to incorporate the term "connected software applications" into 15 CFR 7.1, 7.2, and 7.3 to address the purpose, definition, and scope of covered ICTS transactions. The Department sought public comment on whether it should adjust the definition of

"connected software applications" from the definition in E.O. 14034, or whether the E.O.'s definition sufficiently identifies this category of ICTS transaction.

Drawing from the list of criteria in E.O. 14034 identifying potential indicators of risk the Secretary should consider when assessing whether an ICTS transaction involving connected software applications poses an undue or unacceptable risk, the Department proposed to incorporate these criteria into § 7.103 and requested comments on the usefulness and application of this criteria.

The public comment period for the NPRM initially ended on December 27, 2021, but the Department extended the comment period, at the request of several commenters, to January 11, 2022. The Department received ten comment letters on the NPRM, containing many individual comments. These comments and the Department's responses are addressed below.

II. Response to Comments

Section 7.1 Purpose.

The Department proposed adding the phrase "connected software applications" to 15 CFR 7.1. One commenter supported this addition and suggested that the Department continue to identify other subcategories of ICTS transactions to narrow the scope of ICTS transactions subject to Departmental review. Because the Department interprets E.O. 14034's purpose as only clarifying that connected software applications fall within the existing national emergency regarding the ICTS supply chain, the Department is not identifying other subcategories at this time. The Department has, though, added terms to this provision to clarify that the rule is intended to cover transactions involving ICTS, including connected software applications. In addition, the Department has clarified the types of activities related to connected software applications that the Department believes are important to be covered by the rule. Specifically, the "operation, management, maintenance, or service" of connected software applications by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries could present risks and are therefore covered by the rule.

Additionally, the Department notes that the rule's purpose statement at 15 CFR 7.1 specifically provides that the Secretary may evaluate individual as well as classes of ICTS transactions. Individual transaction reviews are and will remain an important aspect of the Department's authorities, but such reviews may indicate or uncover concerns about more than the single transaction being reviewed, and the Department reiterates that it has the authority to define and review classes of ICTS transactions as well.

Section 7.2 Definitions.

In the NPRM, the Department sought comments on whether the definition of "connected software applications" supplied by E.O. 14034 was sufficient to fully identify this category of ICTS. Commenters generally supported the definition as written. One commenter suggested that the Department delete the word "process" in the definition, reasoning that because the software applications at issue in the rule were "connected," the definition need only cover software applications that can "collect or transmit data." The Department will not change the definition. The word "process" recognizes that there may be national security concerns with connected software applications that process, as well as that collect or transmit, data.

The same commenter felt that the definition's reference to the collection or transmission of data via "the internet" was too restrictive and instead proposed "communication network" as a replacement. The Department will not revise the definition presented in the E.O. However, to provide clarification, this final rule defines "via the internet," for the purposes of this final rule, to mean communicating "using internet protocols to transmit data including, but not limited to, transmissions by cable, telephone line, wireless, satellite or other means."

One commenter wrote that while the reference to "end-point computing device" in the definition was too narrow, "end-point device" should be used rather than "end-to-end technology," and that the Department should include additional devices in the definition. This commenter was concerned that these terms would narrow the definition of connected software applications such that it would not capture devices that are the source and destination point of data in addition to devices

that forward data. Other commenters noted that the term "end-point computing device" might not be technologically accurate, and recommended using another term, such as "end-to-end" to describe what the Department will be regulating.

The Department shares the concerns about an unduly narrow definition that may be technologically inaccurate, and therefore, to avoid confusion and technical inaccuracies, this final rule adds a definition for the term "end-point computing device" to clarify that such device is one that can receive or transmit data and includes as an integral functionality the ability to collect or transmit data via the internet, as that term is defined for the purposes of this final rule.

Section 7.3 Scope of covered transactions.

E.O. 13783 granted the Department authority to review individual as well as certain classes of ICTS transactions, and regulations issued pursuant to that E.O. clarified these classes of transactions as including those involving software, including desktop applications, mobile applications, gaming applications, and web-based applications, designed primarily for connecting with and communicating via the internet that is in use by greater than one million U.S. persons at any point over the twelve months preceding an ICTS transaction. To incorporate the types of software applications that are the subject of E.O. 14034, the Department proposed to add "connected software applications" to this category. One commenter suggested decreasing the user requirements for the software from one million to 250,000 U.S. persons. Though the Department at this time is not considering revisions to the provisions of § 7.3 that contain the user requirement, the Department takes this comment under consideration for potential future revisions to 15 CFR part 7 as the Department gains experience with ICTS involving connected software applications.

Section 7.103 Initial review of ICTS Transactions.

In the NPRM, the Department sought comments on the additions to Part 7 of the criteria laid out in E.O. 14034 regarding how the Department evaluates ICTS transactions involving connected software applications. Specifically, the Department requested comments on whether to modify or add criteria to assist the Department's review of ICTS transactions with connected software applications.

The Department also sought input on whether the Department should use the E.O. 14034 criteria in its review of all ICTS transactions, rather than just those related to connected software applications.

Many commenters supported applying these criteria more broadly to all ICTS transactions. One of these commenters argued that incorporating these criteria into the Department's review of all ICTS transactions would streamline the regulation because ICTS transactions involving connected software applications are a subset of other ICTS transactions. Another commenter disagreed and suggested that the Department should not incorporate these criteria into its review of all ICTS transactions because different standards of review for different types of transactions are necessary given the diversity and complexity of the ICTS supply chain.

The Department has determined that not all of the criteria in E.O. 14034 are applicable to transactions not involving connected software applications. For example, the criterion regarding third-party auditing of connected software applications may not be appropriate to use in evaluating other ICTS transactions or classes of transactions because auditing may not be applicable in those instances. Similarly, the number of users might not be an appropriate factor for evaluating ICTS transactions that have low numbers of users but that service critical infrastructure or that might have significant risks if misused. Additionally, amending the criteria that apply to all ICTS transactions is beyond the scope of this rulemaking as contemplated in E.O. 14034. Therefore, the Department has decided to maintain the approach in the proposed rule and limit the application of these eight new criteria to only those ICTS transactions involving connected software applications.

In the NPRM, the Department also requested comments on additional criteria beyond the proposed eight criteria for evaluating ICTS transactions involving connected software applications. For example, the Department asked whether the software's ability to execute embedded out-going network calls or web server references, regardless of the ownership, control, or management of the software, should be a criterion. Though the Department received one comment in support of this position, other comments were concerned about the potential that this addition would unintentionally capture ICTS transactions, such as those involving call center software and Voice Over Internet

Protocol solutions from domestic vendors. These commenters felt the addition of such a criterion would be unduly broad and disagreed with adding it to the final rule. Commerce agrees with these commenters and is declining at this time to add the criterion. However, as the Department gains experience with ICTS transactions involving connected software applications, the Department may add criteria to these provisions in the future.

Having reviewed these comments, the Department will revise § 7.103 to add the eight criteria enumerated in E.O. 14034, as proposed in the NPRM. The Secretary will use these eight criteria to determine whether ICTS transactions involving connected software applications pose undue or unacceptable risks, as defined in Part 7. In making such decisions, the Secretary will evaluate both the criteria in § 7.103(c), which apply to all ICTS transactions, and the new criteria, which apply specifically to ICTS transactions involving connected software applications. This final rule redesignates current paragraph 7.103(d) as 7.103(e) and adds new paragraph 7.103(d) to include the eight criteria applicable to connected software applications.

Criteria

Below, the Department addresses comments received on each of the eight new criteria taken from E.O. 14034:

1) Ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities.

The Department requested comments on the definition of "ownership, control, or management" as it pertains to the criteria to review connected software applications. Specifically, the Department sought comments on whether this phrase includes or should include both continuous and sporadic "ownership, control, or management." One commenter stated that the scope of the Department's review need not include an evaluation of parties with sporadic access to the software, including, for example, those with access to deploy updates or patches. The commenter believed the Department's scrutiny of such parties could potentially disrupt the frequency of security updates and patches to software applications. The Department understands this concern and does not want to

disrupt necessary security patches and updates. However, the Department is also concerned about the risks, especially to critical infrastructure, posed by sporadic ownership of software applications by malicious cyber actors.

Overall, the Department believes that software security patches or updates for individual consumers typically would not pose risks that rise to the level of requiring the Department's scrutiny. On the other hand, the potential risks to critical infrastructure presented by sporadic access to connected software applications could result in significant harms to the country's infrastructure. The Department is concerned that specifically excluding transactions involving sporadic access to software would create a loophole that would allow exactly the types of malicious cyber acts the rule is meant to prevent. Accordingly, although the Department declines to implement the commenter's suggestion to narrow the definition of "ownership, control, or management" under the rule, the Department notes that it is not the Department's intent to scrutinize every ICTS transaction involving temporary or sporadic access to software to, for example, provide security updates, but rather to be more targeted in its reviews to address the types of risks identified in E.O. 13873.

2) Use of the connected software application to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data.

The Department did not receive comments to this criterion and adds it to part 7 as proposed.

3) Ownership, control, or management of connected software applications by persons subject to coercion or cooption by a foreign adversary.

One commenter suggested that the Department further establish how a person could be found "subject to coercion or cooption," and felt that it might prove difficult for one party to an ICTS transaction to identify the likelihood that the other party is or has been coerced or coopted by a foreign adversary. The Department agrees and, as a result, will align the risk calculation in this criterion with that used in E.O. 13873. Instead of "subject to coercion or cooption by a foreign adversary," the criterion will read "subject to the jurisdiction or direction of a foreign adversary."

This language strikes the balance between the Department's need to be flexible to investigate future transactions and transacting parties' need for appropriate notice. Furthermore, because the Department interprets E.O. 14034 as clarifying that connected software applications fall within the existing national emergency regarding the ICTS supply chain, this change ensures the scope of the inquiry into ICTS transactions related to connected software applications aligns with the scope and language of E.O. 13873.

4) Ownership, control, or management of connected software applications by persons involved in malicious cyber activities.

The Department did not receive comments on this criterion and will incorporate it as proposed.

5) A lack of thorough and reliable third-party auditing of connected software applications.

Many commenters wrote that the auditing envisioned in this final rule should be a continuous process throughout the development and deployment life cycle of the connected software application, rather than a one-time audit. One commenter suggested that the parties developing the application and the parties implementing the application should be subject to audits. Another commenter raised security and privacy concerns regarding this criterion, arguing that granting access to this data to third-party auditors could introduce additional security and privacy concerns. Although the Department agrees that increased access to the data increases risks that the data could be exploited or otherwise misused, the Department has determined that the benefits to parties of being able to audit and secure their own ICTS transactions outweighs the incremental risk increase that results from reliable third-party auditors accessing a connected software application.

The Department also received a number of comments on the proposed definitions of "reliable third-party" and "independently verifiable measures." One commenter suggested that the final rule should explicitly reference established standards or frameworks that parties could use when auditing this data, such as the standards and frameworks in SOC 2 (a compliance standard for service organizations developed by the American Institute of Certified Public Accountants), ISO/IEC

207001 (a set of standards on information security management published by the International Organization for Standardization and the International Electrotechnical Commission), IEC-62443 (a set of standards adopted by the International Electrotechnical Commission to secure industrial automation and control systems), or FedRamp (the U.S. Government's Federal Risk and Authorization Management Program).

The Department has decided to not reference specific standards or frameworks at this time, though the Department encourages the use of recognized standards by third-party auditors. The Department, however, does not want to mandate one type of standard, to allow parties flexibility to adopt an approach appropriate for their company. Therefore, the Department will determine whether a connected software application transaction has undergone reliable third-party auditing on a case-by-case basis to allow parties to these transactions flexibility to account for technological advances in cybersecurity.

One commenter suggested that the Department clarify how each criterion would apply. To address this, the final rule deletes the words "a lack of" so the criterion now reads "whether there is regular, thorough, and reliable third-party auditing."

6) The scope and sensitivity of the data collected.

One commenter suggested adding references to established guidelines such as NIST Special Publication 800-122 (Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)) and guidelines such as ISO/IEC27018:2019 (a publication by the International Organization for Standardization describing a code of practice for protection of PII) in this criterion to clarify what the Department deems sensitive data. Upon consideration of the comment, the Department decided to leave the proposed language unchanged. To promote flexibility in accounting for changes in the type and sensitivity of the data collected by connected software applications, the Department declines to refer to specific published guidelines, which might soon become outdated or might not fully characterize the sensitivity of data. We also note that "sensitive personal data" is defined in 15 CFR 7.2.

7) The number and sensitivity of the users of the connected software application.

One commenter wrote that the Department should consider not just active users of a connected software application, but also stored or past users who still may have sensitive data on the application. The Department agrees with this comment and is clarifying that the Department will consider not just active users of a connected software application but also number and sensitivity of the users and the data collected and/or stored by the connected software application in this criterion. Adding this language furthers the objective of this rulemaking to protect all sensitive data on the connected software application, regardless of whether the user is active.

8) The extent to which identified risks have been or can be addressed by independently verifiable measures.

The Department received a comment on this criterion suggesting that identified vulnerabilities be given a specified period of time to remediate and promote timely mitigation. Because different measures will require different timeframes for mitigation to be effective, the Department believes that specifying a remediation timeline in the regulatory text will not be productive for the implementation and enforcement of this rule. Therefore, the Department has decided not to incorporate this commenter's suggestion into the final rule.

III. Comprehensive List of Changes from the Proposed Rule

In response to the comments discussed above, the Department is editing the proposed language in § 7.103(d)(8) to clarify that the Secretary will be evaluating the extent to which identified risks have been or can be "mitigated," rather than "addressed." Specifically, the Department decided to delete "addressed by independently verifiable" and replace with "mitigated using measures that can be verified by independent third parties," which is more precise.

As noted above, the Department added definitions of "via the internet" and "end-point computing device" to clarify those terms and address commenters' concerns about potential technological inaccuracies.

The Department also amended the language of the criteria, based on public comments. In criterion 3, regarding ownership and control, the Department changed the phrase "subject to coercion or cooption by a foreign adversary," to "subject to the jurisdiction or direction of a foreign adversary" to clarify the criterion. Additionally, the Department removed from the criterion on third-party auditors the words "lack of" and replaced that term with the phrase "whether there is regular, thorough, and reliable third-party auditing" in order to clarify the Department's concern regarding such auditing. Finally, the Department added to criterion 7 regarding the number and sensitivity of users the term "with access to" in order to clarify that the criterion applies to any users that have access to the application.

Classification

A. Executive Order 12866 (Regulatory Policies and Procedures)

Pursuant to the procedures established to implement Executive Order 12866, the Office of Management and Budget has determined that this rule is significant.

B. Regulatory Flexibility Analysis

In the proposed rule, the Chief Counsel for Regulation in the Department of Commerce certified that the rule would not have a significant economic impact on a substantial number of small entities. The factual basis for this certification is contained in the proposed rule and is not repeated here. We received no comments from the public on this certification, and we have no new information about this rule's potential impact on small entities. Accordingly, a final regulatory flexibility analysis was not required, and none was prepared.

C. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.) (PRA) provides that an agency generally cannot conduct or sponsor a collection of information, and no person is required to respond to nor be subject to a penalty for failure to comply with a collection of information, unless that collection has obtained Office of Management and Budget (OMB) approval and displays a

currently valid OMB Control Number. This proposed rule does not contain a collection of information requirement subject to review and approval by OMB under the PRA.

D. Executive Order 13175 (Consultation and Coordination with Indian Tribes)

The Department has analyzed this proposed rule under Executive Order 13175 and has determined that the action would not have a substantial direct effect on one or more Indian tribes, would not impose substantial direct compliance costs on Indian tribal governments, and would not preempt tribal law.

E. National Environmental Policy Act

The Department has reviewed this rulemaking action for the purposes of the National Environmental Policy Act (42 U.S.C. § 4321 et. seq). It has determined that this proposed rule would not have a significant impact on the quality of the human environment.

List of Subjects in 15 CFR Part 7

Administrative practice and procedure, Business and industry, Communications, Computer technology, Critical infrastructure, Executive orders, Foreign persons, Investigations, National security, Penalties, Technology, Telecommunications.

For reasons stated in the preamble, the Department of Commerce amends 15 CFR part 7 as follows:

PART 7 - SECURING THE INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES SUPPLY CHAIN

1. The authority citation for part 7 is revised to read as follows:

Authority: 50 U.S.C. 1701 *et seq.*; 50 U.S.C. 1601 *et seq.*; E.O. 13873, 84 FR 22689; E.O. 14034, 86 FR 31423

2. Revise § 7.1 to read as follows:

§ 7.1 Purpose.

(a) This part sets forth the procedures by which the Secretary may:

(1) Determine whether any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including but not limited to connected software applications, (ICTS Transaction) that has been designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries poses certain undue or unacceptable risks as identified in the Executive Order. For purposes of these regulations, the Secretary will consider ICTS to be designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction of a foreign adversary where such a person operates, manages, maintains, or services the ICTS;

(2) Issue a determination to prohibit an ICTS Transaction;

(3) Direct the timing and manner of the cessation of the ICTS Transaction;

(4) Consider factors that may mitigate the risks posed by the ICTS Transaction.

(b) The Secretary will evaluate ICTS Transactions under this rule, which include, but are not limited to, classes of transactions, on a case-by-case basis. The Secretary, in consultation with appropriate agency heads specified in Executive Order 13873 and other relevant governmental bodies, as appropriate, shall make an initial determination as to whether to prohibit a given ICTS Transaction or propose mitigation measures, by which the ICTS Transaction may be permitted. Parties may submit information in response to the initial determination, including a response to the initial determination and any supporting materials and/or proposed measures to remediate or mitigate the risks identified in the initial determination as posed by the ICTS Transaction at issue. Upon consideration of the parties' submissions, the Secretary will issue a final determination prohibiting the transaction, not prohibiting the transaction, or permitting the transaction subject to the adoption of measures determined by the Secretary to sufficiently mitigate the risks associated with the ICTS Transaction. The Secretary shall also engage in coordination and information sharing, as appropriate, with international partners on the application of this part.

3. In § 7.2, add in alphabetical order definitions for “Connected software application” and “End-point computing device”, revise the definition of “Information and communications technology or services or ICTS” and add in alphabetical order a definition for “Via the internet” to read as follows:

§ 7.2 Definitions.

* * * * *

Connected software application means software, a software program, or a group of software programs, that is designed to be used on an end-point computing device and includes as an integral functionality, the ability to collect, process, or transmit data via the internet.

* * * * *

End-point computing device means a device that can receive or transmit data and includes as an integral functionality the ability to collect or transmit data via the internet.

* * * * *

Information and communications technology or services or ICTS means any hardware, software, including connected software applications, or other product or service, including cloud-computing services, primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means (including electromagnetic, magnetic, and photonic), including through transmission, storage, or display.

* * * * *

Via the internet means using internet protocols to transmit data, including, but not limited to, transmissions by cable, telephone lines, wireless methods, satellites, or other means.

4. In § 7.3:

a. Revise paragraph (a)(4)(v) introductory text;

b. Remove the word “and” in paragraph (a)(4)(v)(C);

c. Remove the word “or” and add the word “and” in its place in paragraph (a)(4)(v)(D); and

d. Add paragraph (a)(4)(v)(E).

The revision and addition read as follows:

§ 7.3 Scope of covered ICTS Transactions.

(a) * * *

(4) * * *

(v) Software designed primarily to enable connecting with and communicating via the internet, which is accessible through cable, telephone line, wireless, or satellite or other means, that is in use by greater than one million U.S. persons at any point over the twelve (12) months preceding an ICTS Transaction, including:

* * * * *

(E) Connected software applications; or

* * * * *

5. In § 7.103, redesignate paragraph (d) as paragraph (e) and add new paragraph (d) to read as follows:

§ 7.103 Initial review of ICTS Transactions.

* * * * *

(d) For ICTS Transactions involving connected software applications that are accepted for review, the Secretary’s assessment of whether the ICTS Transaction poses an undue or unacceptable risk may be determined by evaluating the criteria in paragraph (c) as well as the following additional criteria:

(1) Ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities;

(2) Use of the connected software application to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data;

(3) Ownership, control, or management of connected software applications by persons subject to the jurisdiction or direction of a foreign adversary;

(4) Ownership, control, or management of connected software applications by persons involved in malicious cyber activities;

(5) Whether there is regular, thorough, and reliable third-party auditing of connected software applications;

(6) The scope and sensitivity of the data collected;

(7) The number and sensitivity of the users with access to the connected software application; and

(8) The extent to which identified risks have been or can be mitigated using measures that can be verified by independent third parties.

* * * * *

Alan F. Estevez

Under Secretary of Commerce for Industry and Security
U.S. Department of Commerce

[FR Doc. 2023-12925 Filed: 6/15/2023 4:15 pm; Publication Date: 6/16/2023]